TCP/IP
Solutions Unit Test 1 and Unit 1
==========
==========
Q.1)a)Draw and explain TCP/IP Protocol Architecture.
Ans:

The TCP/IP protocol suite maps to a four-layer conceptual model known as the DARPA model, which was named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer OSI model.
Figure shows the architecture of the TCP/IP protocol suite. The TCP/IP protocol suite has two sets of protocols at the Internet layer: IPv4, also known as IP, is the Internet layer in common use today on private intranets and the Internet. IPv6 is the new Internet layer that will eventually replace the existing IPv4 Internet layer.

Network Interface Layer: The Network Interface Layer (also called the Network Access Layer) sends TCP/IP packets on the network medium and receives TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. Therefore, you can use TCP/IP to communicate across differing network types that use LAN technologies – such as Ethernet and 802.11 wireless LAN – and WAN technologies – such as Frame Relay and Asynchronous Transfer Mode (ATM). By being independent of any specific network technology, TCP/IP can be adapted to new technologies. The Network Interface layer of the DARPA model encompasses the Data Link and Physical layers of the OSI model. The Internet layer of the DARPA model does not take advantage of sequencing and acknowledgment services that might be present in the Data Link layer of the OSI model. The Internet layer assumes an unreliable Network Interface layer and that reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of either the Transport layer or the Application layer.
Internet Layer: The Internet layer responsibilities include addressing, packaging, and routing functions. The Internet layer is analogous to the Network layer of the OSI model. The core protocols for the IPv4 Internet layer consist of the following:
The Address Resolution Protocol (ARP) resolves the Internet layer address to a Network Interface layer address such as a hardware address.

The Internet Protocol (IP) is a routable protocol that addresses, routes, fragments and reassembles packets. The Internet Control Message Protocol (ICMP) reports errors and other information to help you diagnose unsuccessful packet delivery. The Internet Group Management Protocol (IGMP) manages IP multicast groups.
Transport Layer The Transport layer (also known as the Host-to-Host Transport layer) provides the Application layer with session and datagram communication services. The Transport layer encompasses the responsibilities of the OSI Transport layer. The core protocols of the Transport layer are TCP and UDP. TCP provides a one-to-one, connection-oriented, reliable communications service. TCP establishes connections, sequences and acknowledges packets sent, and recovers packets lost during transmission. In contrast to TCP, UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small

(such as the data that would fit into a single packet), when an application developer does not want the overhead associated with TCP connections, or when the applications or upper-layer protocols provide reliable delivery. TCP and UDP operate over both IPv4 and IPv6 Internet layers.

Application Layer The Application layer allows applications to access the services of the other layers, and it defines the protocols that applications use to exchange data. The Application layer contains many protocols, and more are always being developed. The most widely known Application layer protocols help users exchange information: The Hypertext Transfer Protocol (HTTP) transfers files that make up pages on the World Wide Web.

The File Transfer Protocol (FTP) transfers individual files, typically for an interactive user session.
The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments. Additionally, the following Application layer protocols help you use and manage TCP/IP networks:
The Domain Name System (DNS) protocol resolves a host name, such a www.cisco.com, to an IP address and copies name information between DNS servers.
The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network.
The Simple Network Management Protocol (SNMP) collects and exchanges network management information between a network management console and network devices such as routers, bridges, and servers.
Windows Sockets and NetBIOS are examples of Application layer interfaces for TCP/IP applications.

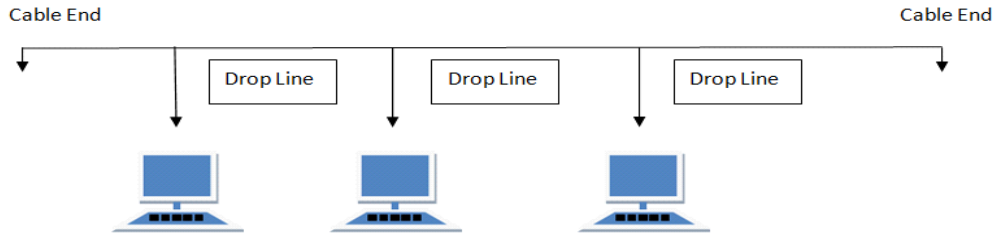
==========

b)Explain in brief Network Topologies.

Ans:

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

- It transmits data only in one direction.
- Every device is connected to a single cable

Advantages of Bus Topology

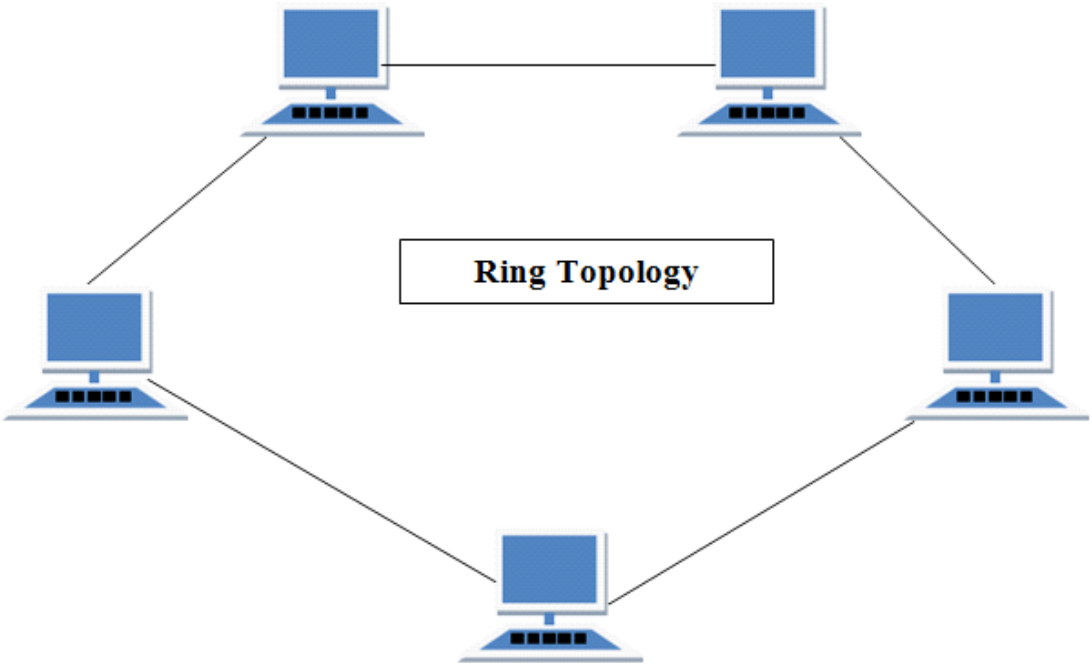
- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

- A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

- In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
- Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

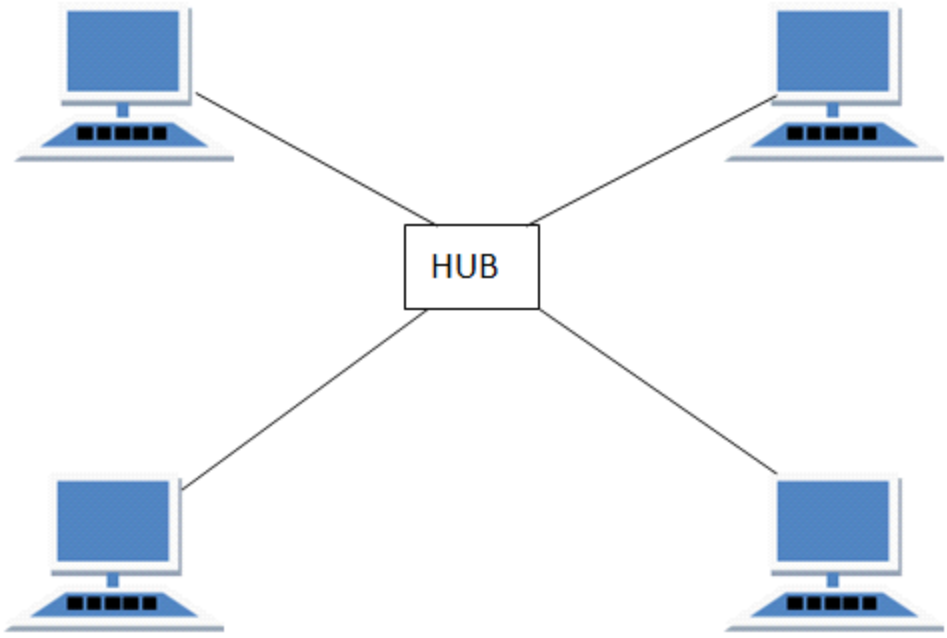
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

Fast performance with few nodes and low network traffic.

- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

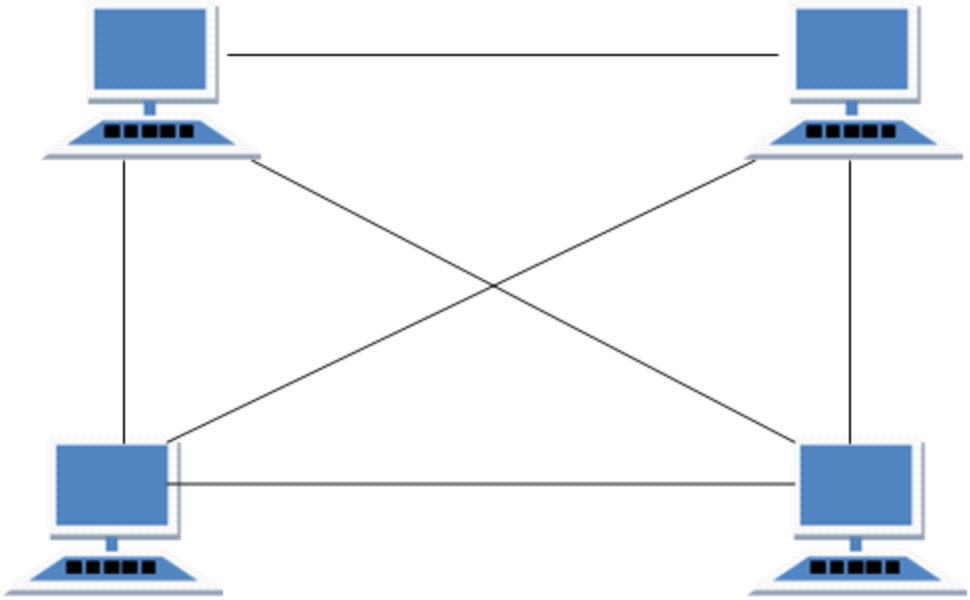
- Routing
- Flooding

Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

- **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
- **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

- Fully connected.
- Robust.
- Not flexible.

Advantages of Mesh Topology

- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

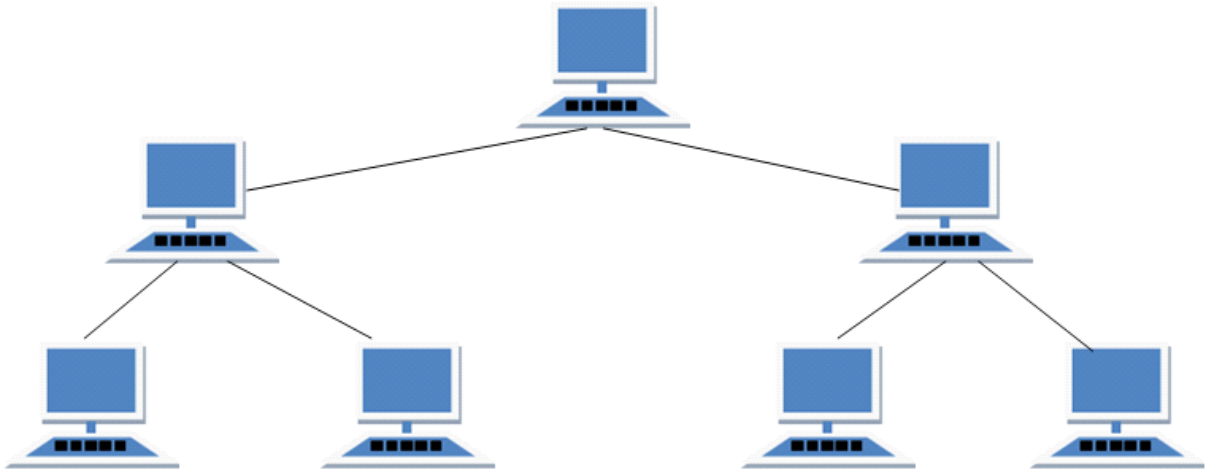
Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called

hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

Ideal if workstations are located in groups.

- Used in Wide Area Network.

Advantages of Tree Topology

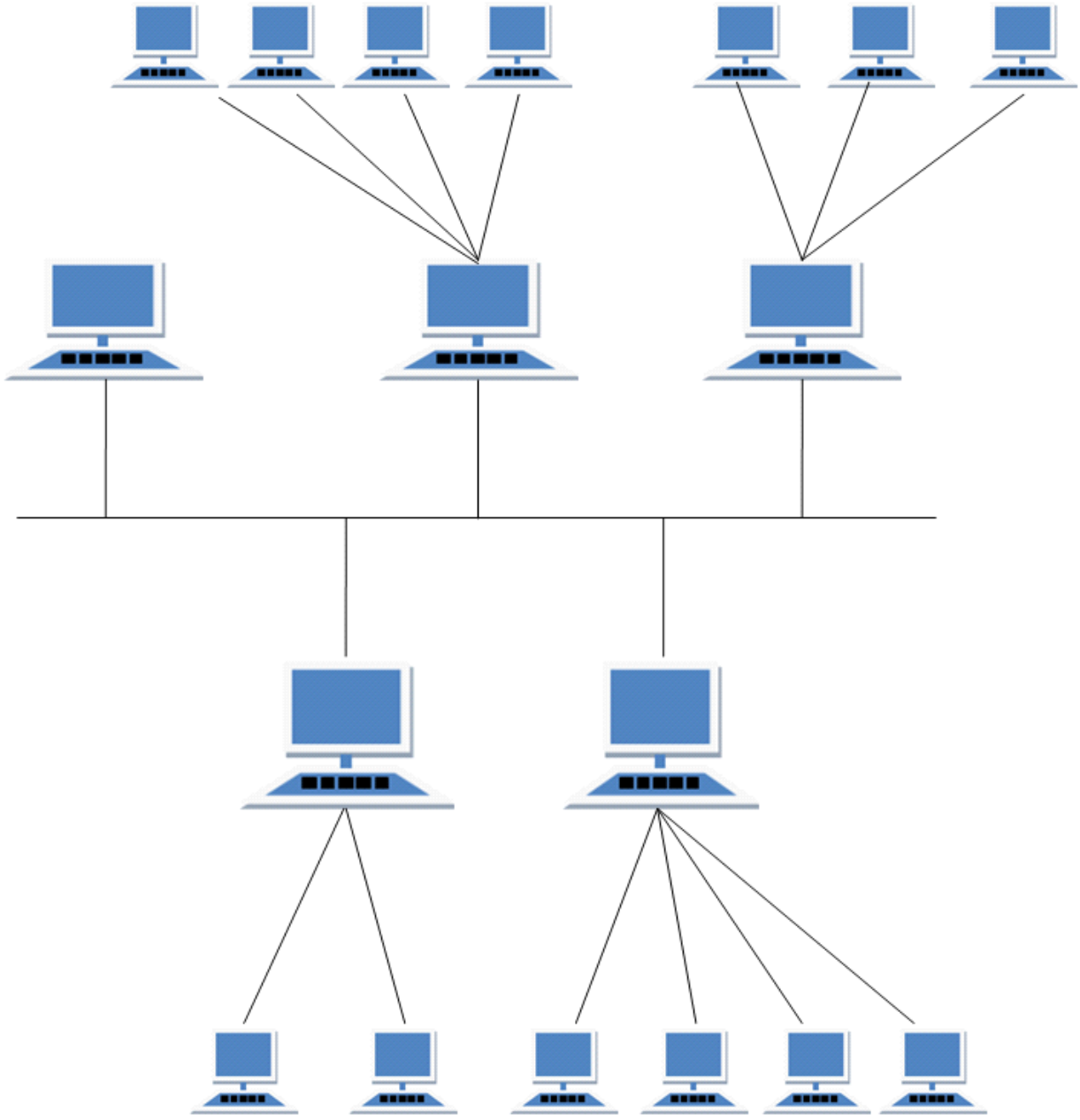
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree Topology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

- It is a combination of two or topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

==========

C)Explain comparison of OSI model and TCP/IP model. Discuss in detail.

Ans:

The OSI Model

Designated ISO/IEC 7498-1, the OSI model is a standard of the International Organization for Standardization (ISO). It is a general-purpose paradigm for discussing or describing how computers communicate with one another over a network. Its seven-layered approach to data transmission divides the many operations up into specific related groups of actions at each layer *(Fig. 1)*.

In the OSI model, data flows down the transmit layers, over the physical link, and then up through the receive layers.

The transmitting computer software gives the data to be transmitted to the applications layer, where it is processed and passed from layer to layer down the stack with each layer performing its designated functions. The data is then transmitted over the physical layer of the network until the destination computer or another device receives it. At this point the data is passed up through the layers again, each layer performing its assigned operations until the data is used by the receiving computer's software.

During transmission, each layer adds a header to the data that directs and indentifies the packet. This process is called encapsulation. The header and data together form the data packet for the next layer that, in turn, adds its header and so on. The combined encapsulated packet is then transmitted and received. The receiving computer reverses the process, de-encapsulating the data at each layer with the header information directing the operations. Then, the application finally uses the data. The process is continued until all data is transmitted and received.

All of the necessary and desirable operations required are grouped together in a logical sequence at each of the layers. Each layer is responsible for specific functions:

• Layer 7 – application: This layer works with the application software to provide communications functions as required. It verifies the availability of a communications partner and the resources to support any data transfer. It also works with end applications such as domain name service (DNS), file transfer protocol (FTP), hypertext transfer protocol (HTTP), Internet message access protocol (IMAP), post office protocol (POP), simple mail transfer protocol (SMTP), Telenet, and terminal emulation.

• Layer 6 – presentation: This layer checks the data to ensure that it is compatible with the communications resources. It ensures compatibility between the data formats at the applications level

and the lower levels. It also handles any needed data formatting or code conversion, as well as data compression and encryption.

• Layer 5 – session: Layer 5 software handles authentication and authorization functions. It also manages the connection between the two communicating devices, establishing a connection, maintaining the connection, and ultimately terminating it. This layer verifies that the data is delivered as well.

Layer 4 – transport: This layer provides quality of service (QoS) functions and ensures the complete delivery of the data. The integrity of the data is guaranteed at this layer via error correction and similar functions.

• Layer 3 – network: The network layer handles packet routing via logical addressing and switching functions.

• Layer 2 – data link: Layer 2 operations package and unpack the data in frames.

• Layer 1 – physical: This layer defines the logic levels, data rate, physical media, and data conversion functions that make up the bit stream of packets from one device to another.

There are two key points to make about the OSI model. First, the OSI model is just that, a model. Its use is not mandated for networking, yet most protocols and systems adhere to it quite closely. It is mainly useful for discussing, describing, and understanding individual network functions.

Second, not all layers are used in some simpler applications. While layers 1, 2, and 3 are mandatory for any data transmission, the application may use some unique interface layer to the application instead of the usual upper layers of the model.

TCP/IP

TCP/IP was developed during the 1960s as part of the Department of Defense's (DoD) Advanced Research Projects Agency (ARPA) effort to build a nationwide packet data network. It was first used in UNIX-based computers in universities and government installations. Today, it is the main protocol used in all Internet operations.

TCP/IP also is a layered protocol but does not use all of the OSI layers, though the layers are equivalent in operation and function *(Fig. 2)*. The network access layer is equivalent to OSI layers 1 and 2. The Internet Protocol layer is comparable to layer 3 in the OSI model. The host-to-host layer is equivalent to OSI layer 4. These are the TCP and UDP (user datagram protocol) functions. Finally, the application layer is similar to OSI layers 5, 6, and 7 combined.

The seven layers of the OSI model somewhat correspond with the four layers that make up the TCP/IP protocol.

The TCP layer packages the data into packets. A header that's added to the data includes source and destination addresses, a sequence number, an acknowledgment number, a check sum for error detection and correction, and some other information *(Fig. 3)*. The header is 20 octets (octet = 8 bits) grouped in 32-bit increments. These bits are transmitted from left to right and top to bottom.

The header is added and then removed during the encapsulation and de-encapsulation of the packet data at the TCP layer.

At the receiving end of the link, TCP reassembles the packets in the correct order and routes them up the stack to the application. TCP can retransmit a packet if an error occurs. In any case, TCP's main job is just to pack and unpack the data and provide some assurance of the reliable transmission of error-free data. The IP layer actually transmits the TCP packet.

The IP layer transmits the data over the physical-layer connection. IP adds its own header to the packet *(Fig. 4)*. The header comprises 32 octets again grouped in 32-bit words. Note the 32-bit source and destination addresses. These are the well-known IP addresses that we see in dotted decimal format (e.g., 197.45.204.36) where each 8-bit octet is expressed in its decimal value. This is the address assigned to the device by the Internet Assigned Numbers Authority (IANA).

The IPv4 header is used during the Internet Protocol process in data transmission. Note the 32-bit source and destination addresses.

The header in Figure 4 is that used in IP version 4 (IPv4). Since the IANA has run out of 32-bit addresses (2^{32} of them!), a newer version is rapidly being adopted. IPv6 uses 128-bit addresses *(Fig. 5)*. With 2^{128} addresses, there should be enough for all of the planet's computers, tablets, and smart phones as well as all of the devices that may be connected to form the so-called Internet of Things (IoT).

The new IPv6 header for the Internet Protocol is similar to IPv4 but uses 128-bit source and destination addresses.

Once the IP header is added to the data, it is transferred to the Network Access layer. This layer repackages the data again into Ethernet packets or some other protocol for final physical transmission. The Ethernet packets are then reconfigured again for transmission over a DSL or cable TV connection or over a wide-area network using Sonet or optical transport network (OTN).

==========

Q.2)a)

What do you mean by internet standards ? Explain in detail.

Ans:

Internet Standard:

The Internet, a loosely-organized international collaboration of autonomous, interconnected networks, supports host-to-host communication through voluntary adherence to open protocols and

procedures defined by Internet Standards. There are also many isolated interconnected networks, which are not connected to the global Internet but use the Internet Standards.

The Internet Standards Process described in this document is concerned with all protocols, procedures, and conventions that are used in or by the Internet, whether or not they are part of the TCP/IP protocol suite. In the case of protocols developed and/or standardized by non-Internet organizations, however, the Internet Standards Process normally applies to the application of the protocol or procedure in the Internet context, not to the specification of the protocol itself.

In general, an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet

The Internet Standards Process

In outline, the process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body (see below), and is published. In practice, the process is more complicated, due to (1) the difficulty of creating specifications of high technical quality; (2) the need to consider the interests of all of the affected parties; (3) the importance of establishing widespread community consensus; and (4) the difficulty of evaluating the utility of a particular specification for the Internet community.

The goals of the Internet Standards Process are:

- o technical excellence;
- o prior implementation and testing;
- o clear, concise, and easily understood documentation;
- o openness and fairness; and
- o timeliness.

The procedures described in this document are designed to be fair, open, and objective; to reflect existing (proven) practice; and to be flexible.

o These procedures are intended to provide a fair, open, and

objective basis for developing, evaluating, and adopting Internet Standards. They provide ample opportunity for participation and comment by all interested parties. At each stage of the standardization process, a specification is repeatedly discussed and its merits debated in open meetings and/or public electronic mailing lists, and it is made available for review via world-wide on-line directories.

- These procedures are explicitly aimed at recognizing and adopting generally-accepted practices. Thus, a candidate specification must be implemented and tested for correct operation and interoperability by multiple independent parties and utilized in increasingly demanding environments, before it can be adopted as an Internet Standard.

- These procedures provide a great deal of flexibility to adapt to the wide variety of circumstances that occur in the standardization process. Experience has shown this flexibility to be vital in achieving the goals listed above.

The goal of technical competence, the requirement for prior implementation and testing, and the need to allow all interested parties to comment all require significant time and effort. On the other hand, today's rapid development of networking technology demands timely development of standards. The Internet Standards Process is intended to balance these conflicting goals. The process is believed to be as short and simple as possible without sacrificing technical excellence, thorough testing before adoption of a standard, or openness and fairness.

From its inception, the Internet has been, and is expected to remain, an evolving system whose participants regularly factor new requirements and technology into its design and implementation. Users of the Internet and providers of the equipment, software, and services that support it should anticipate and embrace this evolution as a major tenet of Internet philosophy.

==========

b) Explain different connecting devices.Also mention the layers of OSI model in which device operates.

Ans:

Hub:

Hub is one of the basic icons of networking devices which works at physical layer and hence connect networking devices physically together. Hubs are fundamentally used in networks that use twisted pair cabling to connect devices. They are designed to transmit the packets to the other appended devices

without altering any of the transmitted packets received. They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

Switches

Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. **Hub** works by sending the data to all the ports on the device whereas a **switch** transfers it only to that port which is connected to the destination device. A switch does so by having an in-built learning of the MAC address of the devices connected to it. Since the transmission of data signals are well defined in a **switch** hence the network performance is consequently enhanced. Switches operate in **full-duplex** mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode. The transmission speed in switches is double than in Ethernet hub transferring a 20Mbps connection into 30Mbps and a 200Mbps connection to become 300Mbps. Performance improvements are observed in networking with the extensive usage of switches in the modern days.

The following method will elucidate further how data transmission takes place via switches:

- **Cut-through transmission**: It allows the packets to be forwarded as soon as they are received. The method is prompt and quick but the possibility of error checking gets overlooked in such kind of packet data transmission.
- **Store and forward**: In this switching environment the entire packet are received and 'checked' before being forwarded ahead. The errors are thus eliminated before being propagated further. The downside of this process is that error checking takes relatively longer time consequently making it a bit slower in processing and delivering.
- **Fragment Free**: In a fragment free switching environment, a greater part of the packet is examined so that the switch can determine whether the packet has been caught up in a collision. After the collision status is determined, the packet is forwarded.

Bridges

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two *segments* of the same LAN that use the same protocol.

Apart from building up larger networks, bridges are also used to segment larger networks into *smaller* portions. The bridge does so by placing itself between the two portions of two physical networks and controlling the flow of the data between them. Bridges nominate to forward the data after inspecting into the MAC address of the devices connected to every segment. The forwarding of the data is dependent on the acknowledgement of the fact that the destination address resides on some other interface. It has the capacity to block the incoming flow of data as well. Today **Learning bridges** have been introduced that build a list of the MAC addresses on the interface by observing the traffic on the network. This is a leap in the development field of manually recording of MAC addresses.

Types of Bridges:

There are mainly three types in which bridges can be characterized:

- **Transparent Bridge:** As the name signifies, it appears to be transparent for the other devices on the network. The other devices are ignorant of its existence. It only blocks or forwards the data as per the MAC address.
- **Source Route Bridge:** It derives its name from the fact that the path which packet takes through the network is implanted within the packet. It is mainly used in Token ring networks.
- **Translational Bridge:** The process of conversion takes place via Translational Bridge. It converts the data format of one networking to another. For instance Token ring to Ethernet and vice versa.

Routers

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process *logical* addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol. It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.

Functionality:

When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

Routing tables play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be *updated* and *complete*. The two ways through which a router can receive information are:

Static Routing: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.

- **Dynamic Routing**: For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

==========

c)What is RFC? Draw and define various maturity levels of RFC.
Ans:

An **Internet Standard** is as thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a six-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment (RFC).** Each RFC is edited, assigned a number, and made available to all interested parties.

RFCs go through maturity levels and are categorized according to their requirement level.

Maturity Levels

An RFC, during its lifetime, falls into one of six **maturity levels:** proposed standard, draft standard, Internet standard, historic, experimental, and Informational.

- **Proposed Standard.** A proposed standard is a specification that is stable, well understood, and of sufficient interest to the internet community**.** At this level, the specification is usually tested and implemented by several different programs.
- **Draft Standard.** A proposed standard is elevated to draft standard status after atleast two successful independent and interoperable implementations. Barring difficulties, a draft standard, with modifications if specific problems are encountered, normally becomes an internet standard.
- **Internet Standard.** A draft standard reaches Internet standard after demonstrations of successful implementation.
- **Historic.** The Historic RFCs are significant from a historical perspective. They either have been superseded by later specifications or have never passed the necessary maturity levels to become an internet standard.
- **Experimental.** An RFC classified as experimental describes work related to an experimental situation that does not affect the operation of the internet. Such an RFC should not be implemented in any functional Internet service.
- **Informational.** An RFC classified as informational contains general, historical, or tutorial information related to the Internet. It is usually written by someone in a non-Internet organization, such as a vendor.